U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY

DOT H 1350.250
May 21, 1999

DEPARTMENTAL GUIDE TO CERTIFICATION/ACCREDITATION OF INFORMATION SYSTEMS

TABLE OF CONTENTS

PURPOSE

Information systems must be given a level of protection commensurate with their importance to the overall Departmental mission and with the mission risks introduced by using this information technology. The importance of the information system is based on both intangibles, such as the value of the information being processed, and tangibles, such as the value of physical facilities. Information systems will be placed into categories, each with its own unique management and security concerns. Information system (IS) security levels are used to define the protection requirements for Department of Transportation (DOT) information and information systems. Once information has been categorized, the appropriate IS security level for that information must be determined. This is required to assure that appropriate protective measures can be are applied This guide provides a detailed approach for certification and accreditation also known as "Approval to Operate". This is required in accordance with Office of Management and Budget (OMB) Circular A-130 Appendix III and the Computer Security Act of 1987 and applies to all General Support Systems or Major Applications.

SCOPE

This guide applies to all information technology (IT) systems or major applications owned, leased, operated or connected to by the Department of Transportation (DOT).

REFERENCES

See DOT 1530.2.1 Definitions and Terms.

BACKGROUND

The Department of Transportation (DOT) on a daily basis uses computer systems to manage, process, transmit and store information related to a broad range of programs. This information is critical to accomplishing the mission of DOT thus its integrity, availability and confidentiality must be assured. The security of DOT general support systems (systems) and major applications (applications) is vital to provide timely and accurate services, deter fraud, waste, and abuse, protect the privacy of individuals, and avoid embarrassment to the Government.

The Certification and Accreditation process is a two-phase process. These processes are:

- CERTIFICATION: Which involves implementation and testing information system security safeguards for a system or application. This process is followed by,

- ACCREDITATION (Authority to Operate): Is the process by which a system owner applies for a formal declaration by an agency official that a system or application meets the applicable Federal policies, regulation and standards. That the implemented security safeguards are adequate to assure the integrity, availability and confidentiality of the information being processed, transmitted or stored consistent with the level of sensitivity of that information.

b. The Certification Process

OMB Circular A-130, Appendix III, requires Federal agencies to establish a process to assure that adequate security is provided for all Departmental information collected, processed, transmitted, stored, or disseminated in systems and applications. This certification process requires:

<u>Security specification:</u> Define and approve security safeguard requirements and specifications prior to starting formal system or application development or procurement.

<u>Design reviews and system tests:</u> Verify that selected / implemented Management, Operational and Technical Controls mitigate those risks which are deemed to be unacceptible.

Certification: Upon completion of the system test, an agency official certifies that the system or application meets applicable Federal policies, regulations and standards, and that the results of the tests demonstrate the installed security safeguards are adequate for the system or application.

Periodic review and re-certification: Agencies are required to conduct periodic audits or reviews of systems or applications and reevaluate the adequacy of security safeguards at least every 3 years. This allows for emerging technologies to be used in the best interest of the Department or Operating Administration (OA).

c. The Accreditation Process

The authorization of a system or application to process, store or disseminate information, granted by a management official, provides an important quality control, the Department refers to this authorization as “Authority to Operate”. By authorizing processing, storage, or dissemination on a system or by an application a manager accepts the risk associated with it. Here there is a distinct difference between a General Support System and a Major Application. The “Authority to Operate” should be reviewed at least every 3 years.

1) General Support Systems: Both the security official and the authorizing management official have responsibilities. In general the security official will direct or perform security tasks, where the authorizing official will normally have general responsibility for the Department or OA supported by the system.

2) Major Application: A major application is authorized by the management official responsible for the function supported by the application. This authorization should be reviewed at least every three years or more often, dependent on the level of risk and magnitude of harm. This review should also take into consideration the risks from the general support systems used by the application or where the application is hosted.

CERTIFICATION

The process for certifying systems or applications should be properly planned, initiated, and managed. This section highlights the steps for this process.

d. **Assign A Project Leader**

A successful certification process starts with the assignment of a certification project leader. The project leader is normally the organization's information systems security officer (ISSO). For new and significantly modified systems or applications, the project leader performs certification work in conjunction with the system application development team.

e. **Initiate A Project Charter**

The security charter includes the scope of work to be performed by the participants, the resources needed, the work plan or schedule, and the sponsor. The project charter is the basis for obtaining formal authorization to proceed, acquiring resources, orienting project participants, and reaching a consensus within the organization of the project scope and context. This document may be part of the overall application development charter.

The project leader should circulate the charter to all organizational components that will be involved in the certification process.

f. **Documentation Review**

The project team reviews existing security documents for the target system or application and those host systems to which the system or application connects to, to help determine safeguards that are in place, planned, or not applicable. These documents include:

1) Security Plan: A computer security plan summarizes security and privacy requirements of the system or application under consideration and describes the controls in place or planned for meeting those requirements. The plan also delineates responsibilities and expected behavior of all individuals who access the system. The OMB recommended format includes four basic sections: System Identification, Management Controls, Operational Controls, and Technical Controls. Security Plans and their content will be discussed in more detail in the accreditation section.

2) Risk Assessment: The analysis of threats, vulnerabilities, assets and safeguards, as they affect systems or applications determines their risk. If the system or application has not had a risk assessment completed, this fact should be cited. The project charter, identified in paragraph 5b above should be expanded to reflect this added need. See DOT 1350.252 "Departmental Guide to Risk Assessment Planning" for a more detailed discussion on risk assessments.

3) System Test and Evaluation (ST&E): The ST&E is a critical element of certification process. This element tests the effectiveness of safeguards that have been implemented to protect the system or application. If a ST&E has been done previously, this document should be reviewed and updated where necessary.

4) Contingency/Disaster Recovery Plan: An existing plan may be updated to meet the requirement. If none exits, it should be documented in the security plan as a "planned" safeguard and included in the Certification/Accreditation Statement as a planned action. See DOT 1350-254

5) Audits, Reviews and Re-Certifications: Systems and applications must be re-certified at least every three years. Review of this documentation may identify limitations on the system or application that may not be general knowledge or detected previously.

6) Management Reviews: These include departmental and OA Information Resource Management (IRM) reviews and related activities.

7) Inspector General (IG) Audit Reviews: The IG conducts several audits and reviews each year, including computer security audits. Review of this documentation may identify limitations on the system or application that may not be general knowledge or detected previously.

8) Systems Life-Cycle Technical Documents: These are prepared to support the development, operation, and maintenance of the system that should be reviewed to support the certification review. These Include among others:

a) Functional Requirements Analysis
b) Design Specifications
c) Hardware and Software Configuration
d) Testing and Acceptance Documentation
e) Systems Manual and User Manual

g. Design Reviews and System Tests and Evaluation

Design reviews and system tests are methods of determining the cost as well as the technical efficiency of safeguards for a system or application. These reviews should be conducted prior to filing for a final “Authority to Operate”. This is to assure that the system or application has made an effort to mitigate their “unacceptible risk” and that the safeguards implemented are mission enhancing and effective.

1) Design Reviews

The purpose of the design review is to ensure that all safeguards have been incorporated into the application system during the design phase.

The purpose of the design phase is to determine how best to satisfy requirements. The primary security goal is to ensure that system requirements are adequately incorporated into the design specifications, including controls that ensure auditability.[1] the design team determines how the system will work, addressing the components, subsystems, and modules. An application system is usually technology environment component that is composed of multiple systems, various hardware, software, and networking elements. Application security must therefore be implemented from a comprehensive, system-wide viewpoint. Components of a major application system may include multiple applications, a database management system (DBMS), a host computer, and a network.

Security requirements may be designed into the system in various ways. For example, authentication control, or passwords, may depend entirely on the operating system controls or a combination of DBMS, computer operating system, and the network operating system controls. When the desired hardware and software combinations do not provide sufficient security, special products may be added to the system, such as RACF or Top Secret for mainframes, WatchDog Director or Net-DAC for networks, or PC-DAC for PC’s.

To facilitate a design review, as required by OMB Circular A-130, the documentation should show where and how the security specifications are implemented. The design review is the last reasonable opportunity to identify weak points in the security plan. Omissions or inadequacies in the security feature if the design that is not identified in the design review may require costly software modifications.

2) SYSTEM TESTS

System testing is the means by which the effectiveness of implemented safeguards can be tested, validated and reported. These test results will also allow managers the ability determine if the return on investment for a specific safeguard is economically feasible.

Testing could include both static and dynamic procedures, such as:

a) Static evaluation techniques which include:

- Conduct of tests for each security safeguard
- Conduct of penetration studies to find security flaws
- Review of code compliance with design specifications

b) Dynamic testing means the operation of the application system with test data and the comparison of the actual results with expected or known results.

c) Specifications, Tests, And Results

Specifications and tests should be as specific as possible. A proven method is to use a specification/test/result process, as illustrated below.

1.	Specification:	Identify sensitive application positions and screen incumbents
	Test Results:	*Sensitive positions are properly identified , but incumbents have not been screened.
2	Specification:	Conduct a risk analysis of the host computer facility.
	Test procedure:	Review the risk analysis documentation for quality and completeness.
	Test results:	* Risk analysis completed 3 years ago, but the facility received major networking capabilities 18 months ago with no risk analysis update.
3	Specification:	Identify and provide security training to all users, technical staff, and management personnel directly involved with this application system.
	Test procedure:	Review training records and spot check five individuals.
	Test results:	* Security awareness training in progress. Training records are incomplete and only two of five individuals received security training.
4	Specification:	Implement a contingency plan for the application system.
	Test procedure:	Review plan for adequacy, including offsite backups, alternate location, and software tests.
	Test results:	* An adequate contingency plan exists, but backups are not stored offsite, and software tests have not been conducted.
5	Specification:	Implement password protection for the application system.
	Test procedure:	Determine whether the password system meets the recommended criteria of FIPS PUB 112 for the designated level of system sensitivity (i.e., medium).
	Test results:	* The password system does not meet minimum guidelines: group passwords exits, a 6-month lifetime for passwords is not enforced, obsolete accounts and passwords are on the system.

In the above samples the five asterisked (*) test results indicate that the specification is not implemented fully. These asterisked test results may affect the certifiability of the system, because OMB requires an agency official to certify that the system meets all applicable Federal policies, regulations and standards, and that the results of the test demonstrate the installed security safeguards are adequate for the application.

These asterisked items should be corrected immediately, if possible, or they should be listed on the certification statement as “restrictions” or “corrective actions.” The process for accomplishing the formal statement is addressed in the next section, Certification.

h. **CERTIFICATION DOCUMENT**

When the certifying officials are satisfied that the system or application has adequate safeguards, a certification report is prepared and a certification statement is signed. When the ST&E is completed this information will be incorporated into the General Support System or Major Application Security Plan. Restrictions and corrective actions are listed on the statement. See the sample Certification Statement on the following page.

If the certifying officials are not satisfied that the application system has adequate safeguards, a deferral certification statement may be executed. A sample Certification Deferral statement is also provided following the certification statement.

SAMPLE GENERAL SUPPORT SYSTEM CERTIFICATION STATEMENT

Dated: (Enter Date Here)

(I / We) certify that having carefully reviewed the following listed documents:

1. (System Name) Security Plan, dated (Enter Date)
2. Risk Assessment, dated (Enter Date)
3. System Test and Evaluation Report, dated (Enter Date)
4. Continuity of Operations Plan, dated (Enter Date)
5. Contingency Plan, dated (Enter Date)
6. Other Ancillary System Documentation
   a. (List by Name and Date of Document) e.g. Network Diagrams,
   b. (List by Name and Date of Document) e.g. System Design Review,
   c. (List by Name and Date of Document) e.g. Rules of Behavior,
   d. (List by Name and Date of Document) e.g. Memorandums of Understanding, etc.

(I / We) certify that the safeguards designed, developed, and implemented (have / have not) reasonably demonstrated through the test results to (provide / not provide) the necessary security to reduce the risk of operating the aforementioned system to an acceptable level.

Based on this review (I / We) (recommend / do not recommend / recommend with comment) that the aforementioned system be submitted for Authority to Operate.

(Restrictions or Comments, if any) (This section can recommend corrective action to be taken to include a schedule for these actions to take place.)

____
(Signature / Title of Certifying Official

____
(Signature / Title of System Owner

____
(Signature / Title of Security Officer)

SAMPLE MAJOR APPLICATION CERTIFICATION STATEMENT

Dated: (Enter Date Here)

(I / We) certify that having carefully reviewed the following listed documents:

1. (Application Name) Security Plan, dated (Enter Date)
2. Risk Assessment, dated (Enter Date)
3. System Test and Evaluation Report, dated (Enter Date)
4. Continuity of Operations Plan, dated (Enter Date)
5. Contingency Plan, dated (Enter Date)
6. Other Ancillary System Documentation
   a. (List by Name and Date of Document) e.g. ERD's
   b. (List by Name and Date of Document) e.g. Application Design Review,
   c. (List by Name and Date of Document) e.g. Rules of Behavior,
   d. (List by Name and Date of Document) e.g. Memorandums of Understanding, etc.

(I / We) certify that the safeguards designed, developed, and implemented (have / have not) reasonably demonstrated through the test results to (provide / not provide) the necessary security to reduce the risk of operating the aforementioned application to an acceptable level.

Based on this review (I / We) (recommend / do not recommend / recommend with comment) that the aforementioned application be submitted for Authority to Operate.

(Restrictions or Comments, if any) (This section can recommend corrective action to be taken to include a schedule for these actions to take place.)

____
(Signature / Title of Certifying Official

____
(Signature / Title of System Owner

____
(Signature / Title of Security Officer)

i. **PERIODIC REVIEWS AND RECERTIFICATION**

Appendix III, OMB Circular A-130 states that:

Review of Security Controls. The security of a system will degrade over time, as the technology evolves and as people and procedures change. Reviews should assure that management, operational, personnel, and technical controls are functioning effectively. Security controls may be reviewed by an independent audit or a self review. The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest patches), and penetration testing can assist in the on-going review of different facets of systems. However, these tools are no substitute for a formal management review at least every three years. Indeed, for some high-risk systems with rapidly changing technology, three years will be too long.

Depending upon the risk and magnitude of harm that could result, weaknesses identified during the review of security controls should be reported as deficiencies in accordance with OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act. In particular, if a basic management control such as assignment of responsibility, a workable security plan, or management authorization are missing, then consideration should be given to identifying a deficiency.

ACCREDITATION PROCESS

The accreditation process is where all the information concerning the system or application is compiled to depict the true status of its security posture. Given that not all risks can be completely mitigated and that some risks will not be addresses because it is economically not efficient to do so, this is where everything about the system or application is discussed. The purpose for this presentation of information is to allow the Authorizing Official the ability to make a sound, well informed determination as to the ability of the system or application to operate, while still ensuring confidentiality, availability and integrity of the information processed, stored or disseminated therein.

j. **THE STEPS**

The accreditation process consists of two basic steps. The goal of the process is to provide to the accreditation or approving authority all the information that is needed to make an informed decision as to the suitability of the system or application to protect the availability, integrity and confidentiality of the information that is processed, stored, or disseminated. The three steps are:

- Document Collection / Review
- Package Preparation / Submission

k. **Document Collection / Review**

The collection and review of many documents is key to completing an accreditation package. These documents will identify the system or application, it's design, associated threats, vulnerabilities, assets, and risks. Additionally, these documents will identify how a system or application will continue to be mission productive in the event of a disaster. These and many more items will aid the approval authority in determining if a system or application can be given an authority to operate. Some of these documents include but are not limited to:

1) Security Plan,

   Special consideration should be paid to the security plan during the review. There are many facets to the plan which must be addressed. There is also a difference between the General Support System Security Plan and the Major Application Security Plan. (See paragraph d and e below)

2) Risk Assessment,

3) System Test and Evaluation Report,

4) Continuity of Operations Plan,

5) Contingency Plan,

6) Other Ancillary Documentation e.g. ERD's, Application Design Review, Rules of Behavior, Memorandums of Understanding, etc.

l. **Package Preparation / Submission**

Once all of the documentation has been reviewed and the reviewing official, security official, and / or management has decided that all of the required documentation is present, and meets the standards set forth in Federal regulations, policies, procedures and standards. Then the information should be forwarded to the Approving Authority for determination as to whether or not Authority to Operate will be granted.

m. **SECURITY PLAN (General Support Systems)**

1) SYSTEM IDENTIFICATION

a) System Name/Title

b) Responsible Organization

c) Information Contact(s)

d) Assignment of Security Responsibility

e) System Operational Status (If more than one status is selected, list which part of the system is covered under each status.)

f) General Description/Purpose

g) System Environment

h) System Interconnection/Information Sharing

i) Applicable Laws or Regulations Affecting the System

j) General Description of Information Sensitivity

2) MANAGEMENT CONTROLS

a) Risk Assessment and Management

b) Review of Security Controls

c) Rules of Behavior (See Appendix A)

d) Planning for Security in the Life Cycle

Determine which phase(s) of the life cycle the system or parts of the system are in. Describe how security has been handled in the life cycle phase(s) that the system is currently in.

e) Authorize Processing

3) OPERATIONAL CONTROLS

a) Personnel Security

b) Physical and Environmental Protection

c) Production, Input / Output Controls

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, software should be listed. In this section, provide a synopsis of the procedures in place that support the system. Below is a sampling of topics that should be reported in this section.

d) Contingency Planning

Briefly describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster were to occur. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix.

e) Hardware and System Software Maintenance Controls

f) Integrity Controls

g) Documentation

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security of the system to include backup and contingency activities, as well as descriptions of user and operator procedures.

h) Security Awareness & Training

i) Incident Response Capability

4) TECHNICAL CONTROLS

a) Identification and Authentication

b) Logical Access Controls

c) Audit Trails

n. **SECURITY PLAN (Major Application)**

1) APPLICATION IDENTIFICATION

a) Application Name/Title

b) Responsible Organization

c) Information Contact(s)

d) Assignment of Security Responsibility

e) Application Operational Status (If more than one status is selected, list which part of the Application is covered under each status.)

f) General Description/Purpose

g) Application Environment

h) Application Interconnection/Information Sharing

i) Applicable Laws or Regulations Affecting the Application

j) General Description of Information Sensitivity

2) MANAGEMENT CONTROLS

a) Risk Assessment and Management

b) Review of Security Controls

c) Rules of Behavior (See Appendix A)

d) Planning for Security in the Life Cycle

Determine which phase(s) of the life cycle the Application, or parts of the Application are in. Describe how security has been handled in the life cycle phase(s) the Application is currently in.

e) Authorize Processing

3) OPERATIONAL CONTROLS

a) Personnel Security

b) Physical and Environmental Protection

c) Production, Input/Output Controls

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, application software should be listed. In this section, provide a synopsis of the procedures in place that support the operations of the application. Below is a sampling of topics that should be reported in this section.

d) Contingency Planning

Briefly describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix.

e) Application Software Maintenance Controls

f) Data Integrity/Validation Controls

g) Documentation

Documentation for a Application includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

h) Security Awareness and Training

4) TECHNICAL CONTROLS

a) Identification and Authentication

b) Logical Access Controls

c) Public Access Controls

If the public accesses the major application, discuss the additional security controls used to protect the integrity of the application and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official agency records. Others might include:

d) Audit Trails

CERTIFICATION AND ACCREDITATION REPORTS

Accrediting officials are the agency officials who have authority to accept a system or application's security safeguards and issue an accreditation statement that records the decision. Within DOT, the accrediting official is known as the Designated Approval Authority (DAA). The DAA must also possess authority to allocate resources to achieve acceptable security and to remedy security deficiencies. Without this authority, such individuals cannot realistically take responsibility for the accreditation decision. In general, this requires the Accreditation Authority to include a senior official and perhaps the line manager for the application in question. For some very sensitive applications, the Senior Executive Officer is appropriate as a DAA. In general, the more sensitive the applications, the higher the DAAs are in an organization. DAAs should consult the agency general counsel to determine their personal liabilities."

o. An Annual Review and Training Session

The ideal way to conduct a re-certification is to hold an annual application system meeting in which management, security, and end-user personnel review the security of the system. This approach provides a way to satisfy both the security needs/updates of the system and the training/orientation needs of the individuals who are associated with the system. The process can be as simple as review the CSSP, item by item, for additions, changes, and deletions. Group members should carefully review current procedures for the following:

1) Authentication and access controls: review current authentication and access procedures to determine whether they meet specifications,

2) Audits/accountability: review current procedures and audits to determine whether they meet specifications, and

3) Backups/contingency planning: review actual copy of contingency plan and status of key items to determine whether they meet specifications.

TABLE V-1: References for Basic Security Functions

This table is extracted from Federal documents to illustrate the major statutory and regulatory references for the basic computer security functions.

Basic Security Functions	Computer Security Act 1987	OMB Circ. A-130	A-123 A-127	FPM	FIRMR	PA/FOIA	NIST Pubs
Policy Implement and maintain security program; assign responsibilities		X			X	X	
Security Plans Identify sensitive system; implement security plans	X				X		800-18
Applications Security Certify applications; re-certify every 3 years. Develop and maintain contingency plans.		X X	X		X X		73, 102 87
Installation Security Conduct risk analysis every 3 years. Prepare acquisition specifications. Maintain disaster recover plans.		X X X	X		X X		31,65 87
Personnel Security Designate sensitive positions and screen incumbents		X		X	X		
Security Awareness and Training Train Federal and contractor personnel.	X	X					800-16
Reporting Report security weaknesses in A-123 Report to President		X	X				

* The Computer Security Act of 1987 is implemented through OMB Bulletins and other regulatory material. NIST Special Publication 800-18 outlines the contents of security plans.

APPENDIX A: RULES OF BEHAVIOR

APPENDIX 1A: RULES OF BEHAVIOR (GENERAL SUPPORT SYSTEM)

Hypothetical Government Agency's (HGA)
Backbone Local Area Network

The rules of behavior contained in this document are to be followed by all users of the HGA Local Area Network (LAN). Users will be held accountable for their actions on the LAN. If an employee violates HGA policy regarding the rules of the LAN, they may be subject to disciplinary action at the discretion of HGA management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

Work at home. HGA Personnel Policy Directive 97-03, dated March 10, 1997, authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home. Any work at home arrangement should:

- be in writing;
- identify the time period the work at home will be allowed;
- identify what government equipment and supplies will be needed by the employee at home, and how that equipment and supplies will be transferred and accounted for;
- identify if telecommuting will be needed and allowed (this issue should be discussed between the requesting organization, Information Resources Management Division (IRMD), and the SECURITY OFFICE; see Dial-in access section below); and
- be reviewed by HGA's personnel office prior to commencement.

Dial-in access. No dial-in access is used to access LAN servers. However, if a justifiable need occurs, the IRM Division Director may authorize dial-in access to a LAN server. It is understood that dial-in access would pose additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, IRMD and the SECURITY OFFICE will regularly review telecommunications logs and HGA phone records, and conduct spot-checks to determine if HGA business functions are complying with controls placed on the use of dial-in lines. All dial-in calls will use one-time passwords.

Connection to the Internet. Some HGA personnel have access to the Internet. Access to the Internet should be closely controlled by the SECURITY OFFICE. HGA divisions, staff managers, and technicians should know that only HGA-authorized Internet connections will be allowed, and that all connections must conform to HGA's security and communications architecture.

Protection of copyright licenses (software) – LAN and PC users are not to download LAN-resident software. Audit logs will be reviewed to determine whether employees attempt to access LAN servers on which valuable, off-the-shelf software resides, but to which users have not been granted access. Audit logs will also show users' use of a "copy" command; this may indicate attempts to illegally download software. Unauthorized copying of PC-based software is also prohibited.

Unofficial use of government equipment – Users should be aware that personal use of information resources – LAN and PC – is not authorized.

Use of passwords – Users are to use passwords of a length specified by the LAN system administrators – a mix of six (6) alpha and numeric characters, they are to keep passwords confidential and are not to share passwords with anyone.

System privileges – Users are given access to the LAN based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

Individual accountability – Users will be held accountable for their actions on the LAN. This is stressed during computer security awareness training sessions

Restoration of service – The availability of the LAN is a concern to all users. All users are responsible for ensuring the restoration of services in the event the LAN is unoperational.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for the HGA Backbone LAN.

______________________________ __________Signature of User
Date

APPENDIX 1-B RULES OF BEHAVIOR (MAJOR APPLICATION)

HYPOTHETICAL GOVERNMENT AGENCY'S (HGA)
FINANCIAL INFORMATION SYSTEM

INTRODUCTION

The following rules of behavior are to be followed by all users of the HGA's Financial Information System (HFIS). The rules clearly delineate responsibilities of and expectations for all individuals with access to the HFIS. Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

RESPONSIBILITIES

The Chief, Financial Information Systems Branch, is responsible for ensuring an adequate level of protection is afforded to the FIS, through an appropriate mix of technical, administrative, and managerial controls. The Branch Chief develops policies and procedures, ensures the development and presentation of user and contractor awareness sessions, and inspects and spot checks to determine that an adequate level of compliance with security requirements exists. The Branch Chief is responsible for periodically conducting vulnerability analyses to help determine if security controls are adequate. Special attention will be given to those new and developing technologies, systems, and applications that can open or have opened vulnerabilities in HGA's security posture.

OTHER POLICIES AND PROCEDURES

The rules are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing HFIS. The rules are consistent with the policy and procedures described in the following directives:

HGA IRM Computer Security Handbook. The newly revised Handbook, dated April 4, 1998, contains computer security guidance on a wide range of topics, i.e., personnel security, incident handling, access control mechanisms. This document contains responsibilities for the SECURITY OFFICE, HGA managers, and users.

HFIS Access Control Management Directive. This directive, dated May 6, 1997, contains responsibilities for HFIS data owners and application administrators.

Draft HFIS Access Control Management Directive. The draft HFIS Access Control Management Directive contains specific responsibilities for the security officer.

Letter for External (non-HGA) Users. A letter for Non-HGA users which transmits the applicable HGA policies should be provided to all non-HGA users while using HFIS, or when using HGA systems and applications in general. These responsibilities should be included in training HGA provides for agency security points of contact, and should be included in interagency agreements or other formal agreements or documents between HGA and other organizations.

APPLICATION RULES

4.1 Work at home. HGA Personnel Policy Directive 97-03, dated March 10, 1997, authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home. Any work-at-home arrangement should:

- be in writing;
- identify the time period the work at home will be allowed;
- identify what government equipment and supplies will be needed by the employee at home, and how that equipment and supplies will be transferred and accounted for;
- identify if telecommuting will be needed and allowed (this issue should be discussed between the requesting organization, Information Resources Management Division (IRMD), and the SECURITY OFFICE; see Section 4.2); and
- be reviewed by HGA's personnel office prior to commencement.

4.2 Dial-in access. The IRM Division Director may authorize dial-in access to HFIS. It is understood that dial-in access poses additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, IRMD and the security office will regularly review telecommunications logs and HGA phone records, and conduct spot-checks to determine if HGA business functions are complying with controls placed on the use of dial-in lines. All dial-in calls will use one-time passwords. If dial-in access is allowed to other applications on the system on which HFIS resides, the managers of those applications should also determine if such access could pose a risk to HFIS data.

4.3 Connection to the Internet. Some HGA personnel have access to the Internet. HGA should ensure that the user authentication required for access is adequate to protect HFIS programs and data. If such access is allowed, HGA should carefully document all external connections to ensure access to HFIS is limited to controlled points of entry.

4.4 Protection of software copyright licenses. All copyright licenses associated with the COTS HFIS software are complied with by HGA personnel, as well as by contractors responsible for developing and maintaining HFIS. HGA requires that all copyright licenses for all PC-based and LAN-based software used by HFIS program personnel and contractor personnel are understood and that these personnel comply with the license requirements. End users, supervisors, and function managers are ultimately responsible for this compliance.

4.5 Unofficial use of government equipment. Users should be aware that personal use of information resources is not authorized.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for the HFIS.

______________________________ __________Signature of User
Date

APPENDIX B: MATRIX OF MINIMUM SECURITY SPECIFICATIONS

APPENDIX B: MATRIX OF MINIMUM SECURITY SPECIFICATIONS

This Appendix is a list of safeguards that fit under controls.

Explanation: This matrix is used to identify a minimum set of safeguards that should be implemented to protect classified and sensitive application systems and general support systems. The safeguards listed below are similar to those listed in Section 4.2.2 of the DOT Guide for Local Area Network (LAN)/Wide Area Network (WAN) Security.

Justification for non-implementation of these safeguards should be based on the results of a formal risk analysis, risk assessment, and cost-benefit analysis.

Directions: Scan the Xs and Os beneath each security level designation. An X means that the security safeguard listed to the left is a requirement. An O means that the security safeguard is optional.

		SECURITY LEVEL			
	CONTROLS	Classified (Level 1)	High Sensitivity (Level 2)	Moderate Sensitivity (Level 2)	Low Sensitivity (Level 2)
	MANAGEMENT CONROLS				
1.	Establish a detailed risk management program	X	X	X	O
2.	Ensure that all personnel positions have been assigned security level designations	X	X	X	X
3.	Conduct periodic security level designation reviews	X	X	X	O
4.	Ensure that all personnel, including contractors, have received appropriate clearances.	X	X	X	O
5.	Maintain a list of all “classified,” “Special-Sensitive,” and “Critical-Sensitive” clearances granted.	X	X	O	O
6.	Conduct formal risk analyses (Host computer/network).	X	X	X	O
7.	Conduct application risk assessment.	X	X	X	X
8.	Prepare and document application rules of behavior	X	X	X	X
9.	Maintain accurate inventory of all hardware and software.	X	X	X	X
SECURITY AWARENESS AND TRAINING					
1.	Establish an employee security awareness and training program.	X	X	X	X
2.	Provide specialized security training	X	X	O	O
DEVELOPMENT/IMPLEMENTATION CONTROLS					
1.	Prepare security specifications.	X	X	X	O
2.	Conduct application design review and system testing.	X	X	X	X
3.	Conduct a security review and prepare a certification report	X	X	X	X
OPERATIONAL CONTROLS					
1.	Ensure that a complete and current set of documentation exists for all	X	X	X	X

		SECURITY LEVEL			
CONTROLS		Classified (Level 1)	High Sensitivity (Level 2)	Moderate Sensitivity (Level 2)	Low Sensitivity (Level 2)
	operating systems.				
2.	Establish controls over the handling of sensitive data, including labeling materials and controlling the availability and flow of data.	X	X	X	O
3.	Require that all sensitive material be stored in a secure location when not in use.	X	X	X	O
4.	Dispose of unneeded sensitive hard copy documents and erase sensitive data from storage media in a manner that will prevent unauthorized use.	X	X	X	O
5.	Prepare and maintain lists of persons authorized to access facilities and automated information systems processing sensitive data.	X	X	X	O
6.	Establish procedures for controlling access to facilities and automated information systems processing sensitive data.	X	X	X	X
7.	Furnish locks and other protective measures on doors and windows to prevent unauthorized access to computer and support areas.	X	X	X	X
8.	Install emergency (panic) hardware on “emergency exit only” doors. Ensure that emergency exits are appropriately marked.	X	X	X	X
9.	Specify fire-rated walls, ceilings, and doors for construction of new computer facilities or modification of existing facilities.	X	X	O	O
10.	Install smoke/fire detection systems with alarms in the computer facility. When feasible, connect all alarms to a control alarm panel within the facility and to a manned guard station or fire station.	X	X	O	O
11.	Install fire suppression equipment in the computer facility that may include area sprinkler systems with protected control valves, and/or fire extinguishers.	X	X	X	O
12.	Provide emergency power shut down controls to shut down AIS equipment and air conditioning systems in the even of fire or other emergencies. Include protective covers for emergency controls to prevent accidental activation.	X	X	X	O
13.	Provide waterproof covers to protect computers and other electronic equipment from water damage.	X	X	O	O
14.	Establish a fire emergency preparedness plan to include training of fire emergency response teams, development and testing of an evacuation plan, and on site orientation visits for the local fire department.	X	X	X	O
15.	Establish contingency plan and information back-up plan.	X	X	X	X
16.	Establish emergency power program	X	X	O	O
17.	Configuration management and application software maintenance	X	X	X	X

		SECURITY LEVEL			
CONTROLS		Classified (Level 1)	High Sensitivity (Level 2)	Moderate Sensitivity (Level 2)	Low Sensitivity (Level 2)
18.	SDLC documentation	X	X	X	O
TECHNICAL CONTROLS					
1.	Require use of current passwords and log on codes to protect sensitive automated information systems data from unauthorized access.	X	X	X	O
2.	Establish procedures to register and protect secrecy of passwords and log on codes, including the use of a non-print, feature.	X	X	X	O
3.	Limit the number of unsuccessful attempts to access an automated information system or a database.	X	X	X	O
4.	Develop means whereby the user’s authorization can be determined. (This may include answer back capability.)	X	X	X	O
5.	Establish an automated audit trail capability to record user activity.	X	X	X	O
6.	Implement methods, which may include the establishment of encryption, to secure data being transferred between two points	X	X	O	O
7.	Ensure that the operating system contains controls to prevent unauthorized access to the executive or control software system.	X	X	X	O
8.	Ensure that the operating system contains controls that separate user and master modes of operations.	X	X	X	O
9.	Record occurrences of non-routine user/operator activity (such as unauthorized access attempts and operator overrides) and report to the organizational ISSO.	X	X	O	O
10.	Ensure that the operating system provides methods to protect operational status and subsequent restart integrity during and after shutdown.	X	X	O	O
11.	Install software feature(s) that will automatically lock out the terminal if it is not used for a predetermined period of lapsed inactive time, for a specified time after normal closing time, or if a password is not entered correctly after a specified number of times.	X	X	X	O
12.	Ensure that the operating system contains controls to secure the transfer of data between all configuration devices.	X	O	O	O
13.	Secure communication lines	X	O	O	O
15.	Ensure that VIRUS protection procedures are in place and users are trained in virus prevention	X	X	X	X
16.	Implement required access control procedures for public use of the system.	X	X	X	X
17.	Review security and effectiveness of FIREWALLS	X	X	X	X
18.	Prepare written authorization for interconnection with other systems and sharing of sensitive information	X	X	X	X

APPENDIX C: DEVELOPING SPECIFICATIONS FOR NEW APPLICATIONS (REQUIREMENTS ANAYSIS)

APPENDIX C: DEVELOPING SPECIFICATIONS FOR NEW APPLICATIONS (REQUIREMENTS ANALYSIS)

OMB requires agencies to “define and approve security requirements and specifications prior to acquiring or starting formal development of the applications.” This appendix describes procedures for evaluating security specifications during the requirement analysis stage for new applications.

Systems development normally progresses through life-cycle stages, such as planning, analysis, construction, and implementation. The requirement analysis stage reveals the detailed data requirements and information processes that must be protected.

ANALYSIS TECHNIQUES

The basic challenge in developing an application system is to understand the interrelationships between the processes and data. In the analysis phase, developers use structured techniques (e.g., graphical models) to breakdown and reorganize the elements of the information system’s organization. The major data flows indicate the inputs and outputs of the system. As the context diagram is constructed, the development team should review the overall sensitivity of the system and its inputs and outputs. The team should annotate the diagram, using abbreviations for confidentiality, integrity and availability (e.g., C, I, and A) and high, medium, or low (e.g., H, M, L). For example, the team must decide how to categorize requisitions, realizing that the unauthorized disclosure of estimated cost data for a major contract could give an unfair advantage to a prospective bidder. As the development work progresses, the team normally adjusts the annotated context diagram, as needed.

DATA FLOW DIAGRAM

The team divides the application system (context diagram) into its major sub-functions, using a data flow diagram This functional decomposition continues, creating as many data flow diagrams as needed, or until a process can no longer are decomposed. As the data flow diagrams are built, the team reviews each process for type and level of sensitivity and annotates the diagrams accordingly.

DATA MODEL

Most application projects require some type of modeling technique to identify and structure the data. A common technique is the entity relationship diagram (ERD). ERDs help to identify groups of information or entities, the attributes or data elements that belong to each entity, and the relationships among the entities. Entities can be any object, for example a place, thing, event or subject, about which information is kept. Entities can also consist of groups of data, such as standard forms, in which information is kept. As the entity relationship diagrams are built, the development team can review each entity and its attributes (data fields) for type and level of sensitivity, and annotate the diagrams accordingly. In the process of grouping data elements within the entities to eliminate redundancy (called normalization), the issue of sensitivity is important. Certain data fields may be highly sensitive, such as vendor bid data, and the team may want to “fence” these data fields by putting them into a separate entity for the implementation of more restrictive security controls.

APPLICATION SECURITY SPECIFICATIONS

Next, review the annotated process and data models to get an overall picture of the sensitivity requirements. Make a summary matrix of the components with high (level 3) or moderate (level 2) sensitivity, confidentiality6, integrity, or availability.

A matrix of the process and data components may look like the following:

TABLE B-1: Matrix of Sensitive Components

COMPONENTS	SENSITIVITY		
	C	I	A
Process Contracts			
Develop RFP	Low	Low	Moderate
Issue RFP	Low	Low	Moderate
Evaluate Bids	High	High	Moderate
Award Contract	High	High	Moderate
Vendor Proposal Data:			
Contract Line Item No.	Low	Low	Moderate
Vendor ID No.	Low	Low	Moderate
Description	High	High	Moderate
Cost	High	High	Moderate
Overall Sensitivity	High	High	Moderate

In this "sample" review, the team determined that the "Evaluate Bids" and "Award Contract" processes and the vendor-supplied description and cost data are the high sensitivity elements in this application system. The other processes and data were judged to have either medium or low sensitivity.

p. **Sample Data and Process Specifications**

- Sample security specifications for the processes described in the above example include:

  1). Separate duties, designate sensitive positions, screen incumbents
  2). Limit access to sensitive processes to authorized persons
  3). Use automated editing, validation, and error-checking controls
  4). Control computer input and output documents and waste paper

- Security specifications for data are designed to protect the application data within the computer. Therefore, the data specifications are access oriented. Some sample specifications for the sensitive data are:

  5). User access controls (read, write, modify, and delete). For example, access will be limited as follows:

Contract supervisor:	Read, write, modify, and delete
Contracting Officer:	Read, write, modify, and delete
Data entry clerk:	Read and write
Database administrator:	Full system access (Contract office employee)
Programmer:	No access to operational system

  6). Encryption capability for files within the application. Note that when cryptographic protection is needed for sensitive unclassified data, Federal agencies are required to use the NIST-approved Data encryption Standard (DES). NIST has validated only hardware and firmware implementations of DES in commercially available security products.

The foregoing sample security specifications provide confidentiality and integrity protections for the processes and data. Availability protection is provided through the development and implementation of emergency, backup, and contingency requirements. A contingency plan is required to ensure that users can continue to perform essential functions in the event their information technology support is interrupted.

q. **Computer System Security Specifications**

The analysis team should now specify the minimum information system security requirements. These safeguards may be at the application level or the database level and some may be at the operating system or network levels, depending on the actual hardware and software configurations that are selected and designed for the system. For example:

1). User identification and authentication controls
2). Password management – length, time expiration
3). Automatic password encryption and non-display feature
4). Automatic log off after three attempts and "timeouts" if no activity for a specified number of minutes
5). User dial-in access controls

r. **Audit Specifications**

Audit controls provide a system monitoring and recording capability to retain or reconstruct a chronological record of system activities such as logon attempts, access to files and changes to data. "In financial applications, a transaction must be capable of being traced from its initiation, though all the intermediate processing steps, to the resulting financial statement. Similarly, information in the financial statements must be traceable to its origin. Such capability is also essential in non-financial systems or applications."[1]

In specifying the audit requirements, the first step is to determine what needs to be audited and when. The goal is to provide a comprehensive and manageable audit program. The audit requirements are therefore grouped as follows for our example:

1). Exception reporting
 a). User logon failures (after three unsuccessful attempts)
 b). Unauthorized transaction attempts

2). Event records – to identify all transactions entering or exiting the application
3). Journal records – to maintain a complete daily backup for an audit history (which may also be part of the contingencies and disaster recovery planning)
 a) Configuration Management

Major application systems are dependent upon system life cycle management, to include configuration management, good programming practices, and effective computer operations procedures. Problems that affect security includes procedural errors and omissions, deliberate traps inserted into code, inadequate testing and documentation, and flaws in the implementation of security controls. Configuration management procedures should include:

1). Peer review of code to ensure conformance to design requirements,
2). Software library controls to limit access to application or system software,
3). Documentation of security-related code to facilitate review and testing,
4). Separation of duties to limit access to operational code,
5). Isolation of critical code for protection and auditing,
6). Procedures to manage different software versions, and
7). Compliance with system development life cycle requirements.

The security specifications become part of the documentation for the requirement analysis, such as the functional requirements and data requirement documents.

[1] NBS Special Publication 500-153, April 1988